

19 BUNDESREPUBLIK  
DEUTSCHLAND



DEUTSCHES  
PATENTAMT

9 12 1915  
Offenlegungsschrift  
DE 44 40 855 A 1

21 Aktenzeichen: P 44 40 855.2  
22 Anmeldetag: 15. 11. 94  
43 Offenlegungstag: 30. 5. 96

51 Int. Cl.<sup>6</sup>:  
H 04 B 1/59  
H 04 B 1/38  
G 07 C 9/00  
// G 07 B 15/00, E 05 B  
47/00, 49/00

DE 44 40 855 A 1

BEST AVAILABLE COPY

71 Anmelder:

Simons, Oliver, 80797 München, DE; Voß, Ludger,  
81675 München, DE

74 Vertreter:

Strehl, Schübel-Hopf, Groening & Partner, 80538  
München

72 Erfinder:

gleich Anmelder

56 Entgegenhaltungen:

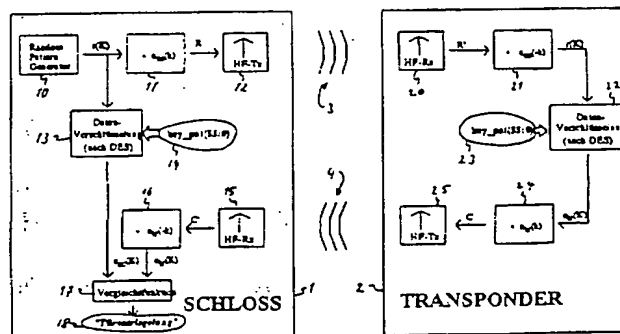
DE 41 34 922 C1  
DE 42 30 011 A1  
DE 41 11 582 A1

Prüfungsantrag gem. § 44 PatG ist gestellt

54 Annäherungssensitives Kontrollsystem

57 Das vorliegende annäherungssensitive Kontrollsystem umfaßt eine Basisstation (Schloß 1) und einen Transponder (2). Bei Annäherung des Transponders (2) an das Schloß (1) wird ein drahtloser Datenaustausch durchgeführt, der dem Schloß (1) die Identifizierung des Transponders (2) ermöglicht. Ergibt die Identifizierung, daß der Transponder (2) zum Schloß (1) paßt, so wird beispielsweise eine Türverriegelung ausgelöst.

Für den Datenaustausch sind sowohl im Schloß (1) als auch im Transponder (2) Sender (12, 25) und Empfänger (15, 20) vorgesehen. Die zu sendenden Daten werden vor dem Senden in Faltungseinrichtungen (11, 24) mit einer Pseudoräuschsequenz gefaltet. Die Daten werden beim Empfang wiedergewonnen, indem die empfangenen Signale in Korrelationseinrichtungen (16, 21) einer Kreuzkorrelation mit der gleichen Pseudoräuschsequenz wie bei der jeweiligen Faltung unterworfen werden. Auf diese Weise wird eine hohe Übertragungssicherheit auch bei sehr geringen Sendeleistungen, miniaturisierten Geräten und Antennen und starken Störeinflüssen möglich. Das verwendete Datenübertragungsprotokoll ist nicht repetitiv und somit abhör- und täuschungssicher. Aufgrund der Signallaufzeit beim Datenaustausch findet eine Messung der Entfernung zwischen Schloß und Transponder statt. Die Türverriegelung wird lediglich dann ausgelöst, wenn sich der Transponder im Nahbereich des Schlosses befindet.



Die folgenden Angaben sind den vom Anmelder eingereichten Unterlagen entnommen

BUNDESDRUCKEREI 04. 96 602 022/61

13/27

Beschreibung

Die Erfindung betrifft ein annäherungssensitives Kontrollsystem sowie eine Basisstation und einen Transponder dafür.

Solche Systeme dienen beispielsweise der automatischen drahtlosen Personen- und Fahrzeugidentifikation bei Verkehrsleitsystemen, der Mautgebührenerfassung, oder der Zutrittskontrolle von Personen und Fahrzeugen zu gesicherten Räumen. Bei der Zutrittskontrolle ersetzen sie mechanische Schließsysteme.

Üblicherweise bestehen annäherungssensitive Kontrollsysteme aus einer Basisstation und einem Transponder. Zwischen diesen beiden Einheiten findet ein drahtloser Datenaustausch statt, der der Basisstation die Identifikation des Transponders ermöglicht. Bei der Zutrittskontrolle löst die Basisstation das Öffnen eines Schlosses aus, sobald sie in der Nähe einen Transponder identifiziert, der einer zutrittsberechtigten Person gehört.

Konventionelle Systeme dieser Art sind mit folgenden Nachteilen behaftet. Zwar haben die Transponder nur etwa die Größe einer Kreditkarte oder eines Schlüsselanhängers, um leicht überallhin mitgeführt zu werden. Die Basisstationen sind demgegenüber jedoch umso größer, um über große Antennen und leistungsstarke Hochfrequenz-Sender und -Empfänger einen sicheren Datenaustausch mit dem Transponder zu ermöglichen. Solche Basisstationen lassen sich wegen ihrer Größe und der erforderlichen Stromzufuhr nicht als Schlösser in konventionelle Türen einbauen.

Idealerweise sollen bei annäherungssensitiven Kontrollsystemen die Basisstation und der Transponder stets eingeschaltet sein, um den Datenaustausch automatisch aufnehmen zu können, sobald sich der Transponder an die Basisstation annähert, ohne daß eine Bedienungsperson eingreifen muß. Der Transponder ist üblicherweise mit winzigen Knopfzellen als Batterien ausgestattet, die jedoch nach kurzer Zeit erschöpft sind. Ein zuverlässiger Betrieb über längere Zeit ist daher mit konventionellen Geräten nicht möglich.

Bei Anwendungen, bei denen der Transponder im fahrenden Fahrzeug mitgeführt wird (beispielsweise Verkehrsleit- oder Kontrollsysteme oder das Öffnen eines Garagentors vom fahrenden Fahrzeug aus), ist die Datenübertragung zwischen konventionellen Basisstationen und Transpondern oft gestört. Beim Einsatz als Ersatz für konventionelle Türschlösser stören sich die Systeme benachbarter Türen aufgrund ihrer Sender gegenseitig.

Der Erfindung liegt daher die Aufgabe zugrunde, einen Transponder und eine Basisstation sowie ein annäherungssensitives Kontrollsystem aus diesem Transponder und dieser Basisstation zu schaffen, die bei kompakten Abmessungen eine sichere Datenübertragung ermöglichen.

Die Lösung dieser Aufgabe gelingt mit dem Transponder nach Anspruch 1 und der Basisstation nach Anspruch 4 sowie den Systemen nach den Ansprüchen 7, 12 und 13.

Der Gegenstand der Ansprüche 1 und 4 beruht auf dem Prinzip, das Transpondersignal, das der Transponder an die Basisstation sendet, um identifiziert zu werden, durch Faltung mit einem vorbestimmten Pseudorandomsignal mit Redundanz zu versehen. Besteht das Signal aus einer Bitsequenz, so bewirkt die Faltung eine Verlängerung der Bitsequenz. Aufgrund der Redundanz läßt sich aus dem gefalteten Signal auch bei sehr geringer Sendeleistung und starken Störungen noch das Transpondersignal zurückgewinnen. Zu diesem Zweck führt die Basisstation eine Kreuzkorrelation des von ihr empfangenen Signals mit dem vorbestimmten Pseudorandomsignal durch.

Vorteilhafte Ausgestaltungen der Erfindung sind in den Unteransprüchen angegeben.

Die Ausgestaltung nach den Ansprüchen 2 und 5 hat den Vorteil, daß auch eine Signalübertragung von der Basisstation an den Transponder mittels eines gefalteten Signals und somit besonders störungsfrei erfolgt. Vorteilhafterweise sendet der Transponder das gefaltete Transpondersignal lediglich dann an die Basisstation, wenn er von ihr vorher ein die zugehörige Basisstation identifizierendes Signal empfangen hat. Durch diese Arbeitsweise wird der Stromverbrauch des Transponders reduziert.

Die Ausführungsformen der Unteransprüche 3 und 6 sind technisch besonders einfach zu realisieren. Die Merkmale des Anspruchs 8 bewirken, daß die Basisstation mit besonders großer Sicherheit lediglich dann ein Verifikationssignal abgibt, wenn sie die Annäherung eines ihr zugeordneten, autorisierten Transponders festgestellt hat. Die übertragenen Signale sind dabei abhörsicher.

Ein weiterer Aspekt der vorliegenden Erfindung ist in Anspruch 12 angegeben. Das System nach Anspruch 12 ermöglicht eine besonders sichere, gegen Mißbrauch geschützte Datenübertragung. Nur wenn Basisstation und Transponder eine gleich arbeitende Verschlüsselungseinrichtung aufweisen, erzeugt die Basisstation das Verifikationssignal. Da das Abfragesignal auf einer Zufallszahlenfolge beruht, läßt sich auch bei heimlichem Abhören der Abfrage- und Antwortsignale keine Information gewinnen, die ein späteres Imitieren des Transponders zur Täuschung der Basisstation ermöglicht. Beim Täuschungsversuch wird die Basisstation ein anderes Abfragesignal als beim vorhergehenden Abhören verwenden, so daß das beim Abhören gewonnene Antwortsignal beim Täuschungsversuch nicht mehr zum Erzeugen eines Verifikationssignals führt.

Ein weiterer Aspekt der Erfindung ist in Anspruch 13 angegeben. Nach diesem System findet zwischen Basisstation und Transponder eine besonders genaue Entfernungsmessung statt, die es ermöglicht, die Annäherung des Transponders an die Basisstation sicher und genau festzustellen. Abhängig von der gemessenen Entfernung kann beispielsweise die Sendeleistung von Transponder und Basisstation eingestellt oder die Entriegelung eines Schlosses erst dann ausgelöst werden, wenn sich die den Transponder tragende Person in unmittelbarer Nähe der Basisstation und damit des Schlosses befindet.

Dadurch wird eine Wechselwirkung zwischen benachbarten Systemen gering gehalten.

Die Signalübertragung zwischen Transponder und Basisstation kann beispielsweise mit elektromagnetischen HF-Wellen, Infrarotstrahlen oder Ultraschall erfolgen.

Die Erfindung hat den Vorteil, daß sie auch bei geringer Antennengröße und kleiner Sendeleistung eine

sichere Signalübertragung zwischen Basisstation und Transponder ermöglicht. Dabei können Transponder und Basisstation mit kleinen Batterien ausgestattet sein, die dennoch auch bei ständig eingeschalteten Geräten eine jahrelange Betriebsdauer ermöglichen. Die Basisstation eignet sich zum Austausch herkömmlicher mechanischer Schlösser in Wohnungs- oder Haustüren. Mit einer Batterie versehen, kann sie netzunabhängig betrieben werden. Wegen der hohen Übertragungssicherheit und der geringen Sendeleistung stören sich Systeme, deren Basisstationen in benachbarte Türen eines Hausflurs eingebaut sind, gegenseitig nicht. Der geringe Stromverbrauch ermöglicht auch den Einsatz in Kraftfahrzeugen. Die Basisstation kann mittels des Verifikationssignals beispielsweise die Kofferraumklappe öffnen, sobald sich der Besitzer mit dem Transponder dem Kraftfahrzeug nähert. Der Besitzer braucht Gegenstände, die er in den Kofferraum legen möchte, vorher nicht abzustellen, um einen Schlüssel oder den Transponder zur Hand zu nehmen. Es ist ausreichend, den Transponder beispielsweise in der Hosentasche mitzuführen.

Ein vorteilhaftes Ausführungsbeispiel der Erfindung wird im folgenden anhand der Zeichnung erläutert. Dabei zeigt

Fig. 1 schematisch den Aufbau des Ausführungsbeispiels, wobei die Basisstation ein Türschloß darstellt und in der Figur der Datenfluß bei Verifikation des Transponders durch das Schloß angegeben ist,

Fig. 2 den schematischen Aufbau einer Einrichtung zur Kreuzkorrelation, und

Fig. 3 den Datenfluß bei Messung der Entfernung zwischen Schloß und Transponder.

Das in Fig. 1 dargestellte Ausführungsbeispiel, bei dem die Basisstation ein Schloß 1 einer Tür darstellt, arbeitet digital. Die Signale sind binäre Bitsequenzen.

Das Schloß 1 ist mit einem Zufallsgenerator 10 zur Lieferung einer 64 Bit langen Zufallssequenz  $r(K)$  versehen,  $K = 1, 2, \dots, 64$ . Die Zufallssequenz wird in einer Faltungseinrichtung 11 mit einer 127 Bit langen Pseudorandomsequenz  $n_{sc}(k)$  bitweise gefaltet,  $k = 1, 2, \dots, 127$ . Das gefaltete Signal R, das eine Länge von  $127 \times 64$  Bit aufweist, wird von einem Sender 12 als Hochfrequenzsignal (im folgenden: Abfragesignal 3) im GHz-Bereich ausgesendet.

Die Zufallssequenz wird außerdem einer Verschlüsselungseinrichtung 13 zugeführt, die mittels eines Verschlüsselungsverfahrens nach DES (Data Encryption Standard, siehe Denning, D.E.; Cryptography and Data Security, Seite 90—101) und eines 56 Bit langen schloßindividuellen Schlüsselwortes, das in einem ROM 14 gespeichert ist, ein Chiffresignal  $c_{sc}(K)$  erzeugt.

In einem Transponder 2 ist ein Empfänger 20 vorgesehen, der das vom Sender 12 kommende Signal als durch Rauschen gestörtes Signal R' empfängt. Das Signal R' wird in der Korrelationseinrichtung 21 einer Kreuzkorrelation mit der Pseudorandomsequenz  $n_{sc}(k)$  unterzogen. Dadurch wird selbst bei hoher Bitfehlerrate auf dem Hochfrequenz-Übertragungsweg wieder die ursprüngliche Zufallssequenz  $r(K)$  zurückgewonnen. Diese wird in der Verschlüsselungseinrichtung 22 verschlüsselt, um ein Chiffresignal  $c_r(K)$  zu bilden. Wenn die Verschlüsselungseinrichtung 22 auf gleiche Weise arbeitet wie die Verschlüsselungseinrichtung 13 des Schlosses und ein in einem ROM 23 des Transponders 2 enthaltenes Schlüsselwort mit dem im ROM 14 des Schlosses enthaltenen Schlüsselwort übereinstimmt, so stimmen auch die beiden Chiffresignale  $c_{sc}(K)$  und  $c_r(K)$  überein. In diesem Fall paßt der Transponder 2 wie ein Schlüssel zum Schloß 1.

Im Transponder 2 wird das Chiffresignal  $c_r(K)$  in einer Faltungseinrichtung 24 mit einer Pseudorandomsequenz  $n_r(k)$  gefaltet. Das durch Faltung erhaltene Signal C wird mittels eines Senders 25 als Hochfrequenzsignal (im folgenden: Antwortsignal 4) vom Transponder 2 an das Schloß 1 gesendet.

Im Schloß 1 befindet sich ein Empfänger 15, der das Signal C als durch Rauschen gestörtes Signal C' empfängt. In einer Korrelationseinrichtung 16 wird das gestörte Signal C' einer Kreuzkorrelation mit der Pseudorandomsequenz  $n_r(k)$  unterworfen, um das vom Transponder erzeugte Chiffresignal  $c_r(K)$  wiederherzustellen. Aufgrund der Kreuzkorrelation gelingt die Wiederherstellung auch bei sehr stark gestörtem Hochfrequenz-Übertragungsweg zwischen Transponder 2 und Schloß 1. Im Schloß 1 ist ein Vergleicher 17 vorgesehen, der das im Transponder 2 erzeugte und von der Korrelationseinrichtung 16 wiederhergestellte Chiffresignal  $c_r(K)$  mit dem von der Verschlüsselungseinrichtung 13 des Schlosses 1 erzeugten Chiffresignal  $c_{sc}(K)$  vergleicht und bei Übereinstimmung ein Verifikationssignal ausgibt. Das Verifikationssignal wird also lediglich dann erzeugt, wenn der Transponder 2 wie oben angegeben zum Schloß 1 paßt. Das Verifikationssignal wird einer Entriegelungseinrichtung 18 zugeführt, die eine elektromagnetische Türetriegelung auslöst. Jede Person, die den passenden Transponder 2 mitführt, wird somit als Zutrittsberechtigter zu der vom Schloß 1 gesicherten Tür angesehen.

Das vorliegende Ausführungsbeispiel ist abhör- bzw. täuschungssicher. Das zu einem bestimmten vom Schloß 1 an den Transponder 2 einer zutrittsberechtigten Person übertragene Abfragesignal 3 sowie das zugehörige vom Transponder 2 an das Schloß 1 übermittelte Antwortsignal 4 lassen sich zwar abhören und abspeichern; bei einem späteren Täuschungsversuch wird der Zufallsgenerator 10 jedoch eine andere Zufallssequenz als beim Abhören erzeugen, so daß sich das aufgezeichnete Antwortsignal 4 nicht zur Türetriegelung verwenden läßt. Da die Zufallssequenz 64 Bit lang ist, ist die Wahrscheinlichkeit, daß sich die Zufallssequenz wiederholt, extrem gering.

Um den schaltungstechnischen Aufwand in der Faltungseinrichtung 11 gering zu halten, wird beim vorliegenden Ausführungsbeispiel die Zufallssequenz nicht als Ganzes mit der Pseudorandomsequenz gefaltet. Statt dessen wird jedes Bit der Zufallssequenz einzeln mit der Pseudorandomsequenz gefaltet. Für jedes Bit mit dem Wert "1" der Zufallssequenz enthält das gefaltete Signal R die Pseudorandomsequenz unverändert; für jedes Bit mit dem Wert "0" enthält das gefaltete Signal die Pseudorandomsequenz in bitweise invertierter Form. Bei einer 64 Bit langen Zufallssequenz und einer 127 Bit langen Pseudorandomsequenz beträgt die Länge des gefalteten Signals  $127 \times 64$  Bit. Die Pseudorandomsequenz wird in der Faltungseinrichtung 11 durch ein geeignet rückgekoppeltes 7-stufiges Schieberegister erzeugt, siehe Golomb, S.W.: Shift Register Sequences.

Die Korrelationseinrichtung 21 arbeitet nach der Autokorrelationsfunktion. Nach Golomb, S.W. Shift Register Sequences gilt für die Autokorrelationsfunktion  $AKF(\tau)$  von Pseudorandomsequenzen  $n(k)$  der Länge L:

$$AKF(\tau) = \sum_{k=1}^L n(k) * n((k + \tau) \bmod L) = \begin{cases} L & \text{für } \tau = 0, \\ -1 & \text{für } (\tau \bmod L) \neq 0, \text{ w } n(k) \in \{+1, -1\} \\ (L-1)/2 & \text{für } (\tau \bmod L) \neq 0, \text{ w } n(k) \in \{0, 1\} \end{cases}$$

Im binären Fall ( $n(k) \in \{0, 1\}$ ) muß  $n(k) \cdot n(k + \tau)$  als Vergleichsoperation, die bei Übereinstimmung von  $n(k)$  und  $n(k + \tau)$  eine 1, bei Abweichung eine 0 liefert, interpretiert werden.

Beim vorliegenden Ausführungsbeispiel entspricht  $n(k)$  der obigen Formel dem Signal R und  $n((k + \tau) \bmod L)$  der Pseudoräuschsequenz  $n_{sc}(k)$ . Enthält die Zufallssequenz  $r(K)$  ein Bit mit dem Wert 1, so nimmt die Funktion  $AKF(\tau)$  für  $\tau = -63, -62 \dots 0, \dots 63$  bei einer Länge der Pseudoräuschsequenz von  $L = 127$  nacheinander die folgenden Werte an:

63, 63, ..., 63, 127, 63, ..., 63

Bei jedem Bit der Zufallssequenz  $r(K)$  mit dem Wert 0 nimmt  $AKF(\tau)$  dagegen folgende Werte an:

64, 64, ..., 64, 0, 64, ..., 64

Die Spitzen (0, 127) der durch Kreuzkorrelation ermittelten Datenfolge  $AKF(\tau)$  geben also die übertragene Information wieder, die im vorliegenden Beispiel aus den Bits der Zufallssequenz besteht.

Bei gestörter Übertragung ( $R' \neq R$ , Signalleistung kleiner Rauschleistung) werden die Spitzenwerte kleiner als 127 bzw. größer als 0 und die übrigen Werte schwanken in einer Bandbreite, die vom Signal/Rauschabstand abhängt, um die Werte 63 bzw. 64. Selbst wenn die Signalenergie nur noch einen kleinen Bruchteil des Rauschens ausmacht, ist noch eine gesicherte Übertragung der Zufallssequenz möglich.

Die Faltungseinrichtung 24 und die Korrelationseinrichtung 16 arbeiten auf gleiche Weise wie die beschriebene Faltungseinrichtung 11 und die Korrelationseinrichtung 21. Sie verwenden jedoch eine andere Pseudoräuschsequenz  $n_{sc}(k)$ , damit benachbarte Schösser sich nicht gegenseitig stören.

Die Korrelationseinrichtungen 16, 21 sind wie in Fig. 2 gezeigt aufgebaut. Sie enthalten ein Schieberegister mit der Länge L der Pseudoräuschsequenz; im vorliegenden Beispiel gilt  $L = 127$  Bit. Jeder der L Schieberegisterpositionen ist ein Bit der Pseudoräuschsequenz 31 zugeordnet. Das Schieberegister 30 weist einen seriellen Eingang 32 auf, dem das Signal  $R'$  bzw.  $C'$  zugeführt wird. Die parallelen Ausgänge des Schieberegisters 30 sind mit einem Addierer 34 verbunden. An denjenigen Schieberegisterpositionen, an denen die zugeordnete Pseudoräuschsequenz eine "1" aufweist, erfolgt die Verbindung direkt; an denjenigen Positionen, an denen die Pseudoräuschsequenz eine "0" aufweist, erfolgt die Verbindung jeweils über einen Inverter 33.

Der Addierer 34 ist mit so vielen Eingängen für jeweils ein Bit versehen, wie Schieberegisterpositionen vorhanden sind. Der Ausgang 36 des Addierers 34 gibt den Wert der Autokorrelationsfunktion an. Zur schnellen und effizienten Berechnung der Summe weist der Addierer eine baumartige Struktur aus Addierermodulen 35 mit jeweils zwei Eingängen und einem Ausgang auf. In der ersten, mit dem Schieberegister 30 verbundenen Ebene der baumartigen Struktur sind die Eingänge der Addierermodule 35 jeweils ein Bit breit. In der zweiten Ebene beträgt die Breite der Eingänge zwei Bit, und in der siebten und letzten Ebene sieben Bit. Der Ausgang 36 des Addierermoduls 35 der letzten Ebene ist ebenfalls sieben Bit breit.

Der Ausgang 36 ist mit einem (nicht dargestellten) Vergleichler verbunden, der den am Ausgang 36 anliegenden Wert der Autokorrelationsfunktion mit einem zwischen 0 und  $(L+1)/2 = 64$  liegenden ersten Schwellenwert und einem zwischen  $(L-1)/2 = 63$  und  $L = 127$  liegenden zweiten Schwellenwert vergleicht. Ist der Wert der Autokorrelationsfunktion kleiner als der erste Schwellenwert, so gibt der Vergleichler ein Bit mit dem Wert "0" aus, während ein Bit mit dem Wert "1" ausgegeben wird, wenn der Wert der Autokorrelationsfunktion größer als der zweite Schwellenwert ist. Die ausgegebenen Bits bilden die im Transponder 2 wiedergewonnene Zufallssequenz  $r(K)$  bzw. die im Schloß 1 wiedergewonnene Chiffresequenz  $c_{tr}(K)$ .

Um sicherzustellen, daß sich eine Zutrittsberechtigte Person (bzw. ihr Transponder) zum Zeitpunkt des Entriegelns der Tür in der Nähe des Schlosses befindet, führt das vorliegende Ausführungsbeispiel eine Distanzmessung zwischen Transponder und Schloß nach Fig. 3 durch. Dazu wird im Schloß 1 die Laufzeit eines zum Transponder gesendeten und vom Transponder (nach Entfaltung durch Kreuzkorrelation und Neufaltung) zurückgegebenen Signals gemessen. Zu diesem Zweck enthält das Schloß einen (nicht dargestellten) Zähler, der mit einem Zählertakt  $f$  von im vorliegenden Beispiel 20 MHz getaktet wird. So erhält man bei einer Lichtgeschwindigkeit von  $c = 300\,000$  km/s eine Entfernungsauflösung von  $c/(2f)$ , im folgenden "Einheitslänge", im vorliegenden Beispiel 7,5 m. Vergrößert man die Entfernung zwischen Transponder und Schloß um 7,5 m, so zählt der Zähler einen 20 MHz Takt mehr, bis das Schloß nach Absenden eines Abfragesignals ein Antwortsignal erhält.

Im Transponder 2 tastet der Empfänger 20 das empfangene Signal mit einer Abtastfrequenz  $ab$ , die etwa ebenso groß ist wie die Frequenz des Zählertakts im Schloß 1. Bei einer kleineren Entfernung zwischen Schloß und Transponder als 7,5 m hängt es von der Phasenbeziehung zwischen Zählertakt im Schloß 1 und Abtasttakt im Transponder 2 ab, ob der Zähler im Schloß eine minimale Taktzahl  $t_0$  (die von der Verarbeitungsgeschwindigkeit der Signale im Transponder abhängt) feststellt, oder einen Takt mehr, also  $t_0 + 1$ .

Die Frequenz des Zählertakts im Schloß 1 und die Abtastfrequenz im Transponder 2 sind geringfügig gegeneinander verstimm, so daß die Phasen beider Takte gegeneinander wandern. Die Entfernungsmessung wird mehrfach (beispielsweise 1024-fach) wiederholt. Die Häufigkeit, mit der der Zähler bei einer Messung  $t_0$

Generalschlüsselebenen werden dadurch realisiert, daß die Zufallssequenz  $r(K)$  in der Verschlüsselungseinrichtung 13 des Schlosses 1 nicht nur entsprechend dem Schlüsselwort des zugehörigen Transponders 2, sondern zusätzlich noch entsprechend dem Schlüsselwort eines oder mehrerer General-Transponder durchgeführt wird. Der ROM 14 enthält dann mehrere Schlüsselworte.

Generalschloßebenen (beispielsweise Wohnungstüren und Haustüren) sind realisiert, indem die Verschlüsselungseinrichtung 22 des Transponders 2 die empfangene und wiedergewonnene Zufallssequenz  $r(K)$  nacheinander entsprechend dem Schlüsselwort des zugehörigen Schlosses 1 sowie dem Schlüsselwort des Generalschlosses (Haustür) verschlüsselt. Diese Schlüsselworte sind im ROM 23 abgelegt.

Der Vergleicher 17 im Schloß 1 prüft, ob mindestens eines der vom Transponder gesendeten Chiffresequenzen  $c_{tr}$  zu einer von der Verschlüsselungseinrichtung 13 gelieferten Chiffresequenzen  $c_{sc}$  paßt. Wenn dies der Fall ist, wird das Verifikationssignal erzeugt.

Der Sender 12 eines Schlosses kann den Empfänger 15 des gleichen oder eines benachbarten Schlosses nicht stören, da für das Senden und Empfangen unterschiedliche Pseudoräuschsequenzen  $n_{sc}$  und  $n_{tr}$  verwendet werden. Gleiches gilt für den Transponder. Beim vorliegenden Ausführungsbeispiel wird der Sender 12 des Schlosses sowohl im Bereitschaftsmodus als auch im aktiven Modus zwischen längeren Pausen nur jeweils kurz betrieben, um Signale auszusenden. Die Einschaltzeit beträgt beispielsweise etwa 1% der gesamten Betriebszeit. Dadurch werden Kollisionen mit benachbarten Systemen vermieden. Kommt es dennoch zu einer Kollision und die Datenübertragung ist gestört, so wird die Übertragung nach einer zufälligen Zeit wiederholt.

Bei der Entfernungsmessung sind die Frequenz des Zählertakts im Schloß 1 und die Abtastfrequenz im Transponder 2 mindestens so weit gegeneinander verstimmt, daß während der Gesamtheit der wiederholten Messungen eine Phasenverschiebung von  $360^\circ$  auftritt und höchstens so weit, daß der genannte Zähler im Schloß 1 bei wiederholten Messungen lediglich zwei verschiedene Zählerstände  $t$  oder  $t + 1$  liefert.

#### Patentansprüche

1. Transponder für ein annäherungssensitives Kontrollsystem, mit einem Transponder-Signalgenerator (20 bis 23, 26) zur Erzeugung eines Transpondersignals, anhand dessen eine Basisstation (1) das Vorhandensein des Transponders (2) erkennen kann, einer Signalfaltungseinrichtung (24) zur Verlängerung des Transpondersignals durch Faltung mit einem vorbestimmten ersten Pseudoräuschsignal, und einem Sender (25) zur drahtlosen Aussendung des gefalteten Signals an die Basisstation (1).
2. Transponder nach Anspruch 1, wobei der Transpondersignalgenerator aufweist: einen Empfänger (20) zum drahtlosen Empfang eines mit einem vorbestimmten zweiten Pseudoräuschsignal gefalteten, verlängerten Basisstationssignals von der Basisstation (1), und eine Korrelationseinrichtung (21) zur Kreuzkorrelation des empfangenen Signals mit dem zweiten Pseudoräuschsignal, um das Basisstationssignal zurückzugewinnen und auf dessen Grundlage die Erzeugung des Transpondersignals zu veranlassen.
3. Transponder nach Anspruch 2, wobei die Signalfaltungseinrichtung (24) für jedes Bit mit dem Wert "1" des Transpondersignals das erste Pseudoräuschsignal und für jedes Bit mit dem Wert "0" des Transpondersignals das bitweise invertierte erste Pseudoräuschsignal ausgibt, und wobei die Korrelationseinrichtung (21) aufweist: ein Schieberegister (30) zur Seriell/Parallel-Umwandlung des empfangenen Signals, dessen einzelne Ausgänge jeweils einem Bit des zweiten Pseudoräuschsignals zugeordnet sind, eine mit dem Schieberegister (30) gekoppelte Additionsschaltung (33 bis 36), die aus zählt, wieviele Bits der Schieberegisterausgänge mit den zugeordneten Bits des zweiten Pseudoräuschsignals übereinstimmen, und eine Erkennungsschaltung, um anhand des Auszählergebnisses ein Bit des Basisstationssignals zu erkennen.
4. Basisstation für ein annäherungssensitives Kontrollsystem, mit einem Empfänger (15) zum drahtlosen Empfang eines mit einem vorbestimmten ersten Pseudoräuschsignal gefalteten, verlängerten Transpondersignals, einer Korrelationseinrichtung (16) zur Kreuzkorrelation des empfangenen Signals mit dem ersten Pseudoräuschsignal, um das Transpondersignal zurückzugewinnen, und einer Einrichtung (16 bis 19) zur Erkennung des Vorhandenseins des Transponders (2) anhand des zurückgewonnenen Transpondersignals.
5. Basisstation nach Anspruch 4, mit einem Basisstations-Signalgenerator (10) zur Erzeugung eines Basisstationssignals, anhand dessen der Transponder (2) das Vorhandensein der Basisstation (1) erkennen kann, einer Signalfaltungseinrichtung (11) zur Verlängerung des Basisstationssignals durch Faltung mit einem vorbestimmten zweiten Pseudoräuschsignal, und einem Sender (12) zur drahtlosen Aussendung des gefalteten Signals an den Transponder (2).
6. Basisstation nach Anspruch 5, wobei die Signalfaltungseinrichtung (11) für jedes Bit mit dem Wert "1" des Basisstationssignals das zweite Pseudoräuschsignal und für jedes Bit mit dem Wert "0" des Basisstationssignals das bitweise invertierte zweite Pseudoräuschsignal ausgibt, und wobei die Korrelationseinrichtung (16) aufweist: ein Schieberegister (30) zur Seriell/Parallel-Umwandlung des empfangenen Signals, dessen einzelne Ausgänge jeweils einem Bit des ersten Pseudoräuschsignals zugeordnet sind, eine mit dem Schieberegister (30) gekoppelte Additionsschaltung (33 bis 36), die aus zählt, wieviele Bits der

Takte im Verhältnis zur Gesamtzahl der Messungen zählt, gibt an, in welchem Teilbereich einer Einheitslänge sich der Transponder von dem Schloß entfernt befindet.

Allgemein gilt für die Entfernung  $D$  zwischen Schloß und Transponder:

$$D = \left\{ \frac{N_t + 1}{N_t + N_{t+1}} + (t - t_0) \right\} \frac{c}{2f}$$

Dabei sind  $t_0$  der gemessene Zählerstand bei  $D = 0$ ,  $t$  und  $t + 1$  die am häufigsten gemessenen Zählerstände bei der momentanen Entfernung zwischen Transponder und Schloß,  $N_t$  und  $N_{t+1}$  die Anzahl der Messungen mit den Zählerständen  $t$  und  $t + 1$ ,  $c$  die Lichtgeschwindigkeit und  $f$  die Frequenz des Zählertakts.

Innerhalb der geschweiften Klammer gibt der zweite Summand die Anzahl der Einheitslängen und der erste Summand den Teilbereich innerhalb einer Einheitslänge an. Beim vorliegenden Ausführungsbeispiel wird für  $t \neq t_0$ , d. h. für Entfernungen über der Einheitslänge von 7,5 m, lediglich der zweite Summand und für  $t = t_0$ , d. h. für kleinere Entfernungen als die Einheitslänge von 7,5 m, lediglich der erste Summand ausgewertet. Diese Vorgehensweise hat den Vorteil, daß für größere Entfernungen keine wiederholten Messungen mit Bestimmung der Häufigkeiten  $N_t$  und  $N_{t+1}$  notwendig sind.

Fig. 3 zeigt den Datenfluß im Schloß 1 und Transponder 2 bei Durchführung der zuvor beschriebenen Entfernungsmessung. Gleiche Einrichtungen wie in Fig. 1 sind mit gleichen Bezugsziffern bezeichnet. Während der Entfernungsmessung nicht benötigte Einrichtungen sind aus Gründen der Übersichtlichkeit nicht dargestellt.

Für jede Entfernungsmessung sendet der Sender 12 des Schlosses 1 einmal die Pseudorandomsequenz  $n_{sc}(k)$  aus. Diese wird von der Faltungseinrichtung 11 erzeugt, wenn an ihrem Eingang ein Bit mit dem Wert "1" anliegt. Der Transponder arbeitet wie bei Fig. 1 erläutert, wobei die Verschlüsselungseinrichtung jedoch mittels einer Direktleitung 26 vom Ausgang der Korrelationseinrichtung 21 zum Eingang der Faltungseinrichtung 24 überbrückt ist.

Im Schloß 1 wird das vom Transponder gelieferte Hochfrequenzsignal vom Empfänger 15 empfangen. Die Faltungseinrichtung 16 erzeugt daraus ein Bit, das wiederum den Wert "1" aufweist. Dieses Bit wird an eine Einheit 19 zur Laufzeitermittlung weitergegeben. Die Einheit 19 bestimmt für wiederholte Messungen, d. h. wiederholtes Aussenden der Pseudorandomsequenz  $n_{sc}(k)$  durch das Schloß 1 die Werte  $t$ ,  $N_t$  und  $N_{t+1}$  und berechnet daraus die Entfernung  $D$ .

Alternativ kann die Entfernungsmessung auch anhand der vom Schloß 1 empfangenen Signalintensität erfolgen. Diese nimmt quadratisch mit der Entfernung zwischen Schloß und Transponder ab, was sich in der Korrelationseinrichtung 16 dadurch bemerkbar macht, daß die Spitzenwerte der Autokorrelationsfunktion kleiner als 127 (für ein übertragenes Bit mit dem Wert "1") bzw. größer als 0 (für ein übertragenes Bit mit dem Wert "0") werden. Anhand von Schwellenwerten läßt sich zwischen Nah- und Fernbereichen unterscheiden.

In einer weiteren Modifikation des Ausführungsbeispiels kann am Schloß ein Schalter (Taster) angebracht sein, und das Schloß führt lediglich dann eine Zutrittsverifikation nach Fig. 1 durch, wenn der Taster von der den Transponder tragenden Person betätigt wird. Eine Entfernungsmessung ist dann überflüssig.

Transponder und Schloß sind mit Batterien versehen. Es ist jeweils eine Batteriespannungs-Überwachungseinrichtung vorhanden, die bei absinkender Spannung der Schloß- bzw. Transponder-Batterie ein Entriegeln der Tür erst nach Betätigung eines Tasters am Schloß bzw. am Transponder, vorzugsweise nach einer Verzögerungszeit von z. B. drei Sekunden auslöst.

Zur Minimierung des Energieverbrauchs arbeiten beim vorliegenden Ausführungsbeispiel Schloß und Transponder in zwei unterschiedlichen Betriebsmodi. Im Bereitschaftsmodus werden beide mit einer sehr langsamen Frequenz getaktet (beispielsweise 10 kHz), im aktiven Modus mit einer schnellen Frequenz (beispielsweise 20 MHz). Im Bereitschaftsmodus sendet das Schloß 1 von Zeit zu Zeit, beispielsweise im Abstand von zwei Sekunden, jeweils eine einfache Pseudorandomsequenz  $n_{sc}(k)$ . Sobald der Transponder 2 diese Sequenz empfängt, sendet er seinerseits die Pseudorandomsequenz  $n_{tr}(k)$  und schaltet in den aktiven Modus. Nach Empfang der vom Transponder gesendeten Pseudorandomsequenz schaltet das Schloß 1 ebenfalls in den aktiven Modus.

Dann sendet das Schloß 2 zunächst eine mit der Pseudorandomsequenz gefaltete schloßindividuelle Identifizierungsnummer. Der Transponder 2 prüft, ob die empfangene Nummer die Identifizierungsnummer seines zugehörigen Schlosses oder eines Generalschlosses ist, zu dem er Zutritt hat. In diesem Fall sendet er die Identifizierungsnummer (wiederum mit seiner Pseudorandomsequenz gefaltet) zurück, andernfalls geht er wieder in den Bereitschaftsmodus.

Bei Anwesenheit mehrerer Schlösser bleibt lediglich das Schloß im aktiven Modus, das seine Identifizierungsnummer von einem Transponder zurückerhalten hat. Das im aktiven Modus verbleibende Schloß und der im aktiven Modus verbleibende Transponder führen sodann eine Entfernungsmessung wie bei Fig. 3 beschrieben durch. Wenn sich der Transponder im unmittelbaren Nahbereich der Tür befindet, erfolgt die Zutrittsberechtigungsverifikation wie bei Fig. 1 beschrieben.

Der beschriebene Betrieb ermöglicht ein berührungsloses Entriegeln des Schlosses, bedeutet aber, daß der Sender 12 des Schlosses 1 von Zeit zu Zeit eine Pseudorandomsequenz aussenden muß, um festzustellen, ob sich ein Transponder nähert. Beim vorliegenden Beispiel, bei dem die Taktfrequenz im Bereitschaftsmodus 10 kHz und die Länge einer Pseudorandomsequenz 127 Bit beträgt, ist der Sender 12 alle zwei Sekunden für 12,7 ms in Betrieb.

Um den damit verbundenen Energieverbrauch zu vermeiden, besteht die Möglichkeit, das Schloß 1 ganz abzuschalten und erst durch Druck oder Zug auf einen im Türknauf vorgesehenen Schalter (Taster) kurz einzuschalten, was die Tür entriegelt, wenn der Transponder in der Nähe ist.

Schieberegisterausgänge mit den zugeordneten Bits des zweiten Pseudoräuschsignals übereinstimmen, und eine Erkennungsschaltung, um anhand des Auszählergebnisses ein Bit des Basisstationssignals zu erkennen.

7. Annäherungssensitives Kontrollsystem mit einem Transponder nach einem der Ansprüche 1 bis 3 und einer Basisstation nach einem der Ansprüche 4 bis 6.

8. Annäherungssensitives Kontrollsystem mit einem Transponder nach einem der Ansprüche 2 und 3 und mit einer Basisstation nach einem der Ansprüche 5 und 6, wobei der Basisstations-Signalgenerator einen Zufallszahlfolgegenerator (10) enthält, der eine Zufallszahlfolge als Basisstationssignal erzeugt,

die Basisstation eine erste Verschlüsselungseinrichtung (13, 14) zur Verschlüsselung der Zufallszahlfolge enthält,

der Transponder-Signalgenerator eine zweite Verschlüsselungseinrichtung (22, 23) zur Verschlüsselung des vom Transponder empfangenen und durch Kreuzkorrelation rückgewonnenen Basisstationssignals und zur Erzeugung des Transpondersignals enthält, und

die Basisstation eine Verifikationseinrichtung (17) zum Vergleich der von der ersten Verschlüsselungseinrichtung (13, 14) erzeugten verschlüsselten Zufallszahlfolge mit dem von der Basisstation (1) rückgewonnenen Transpondersignal, um bei Übereinstimmung ein Verifikationssignal auszugeben, enthält.

9. System nach Anspruch 8, wobei die Basisstation eine Entriegelungseinrichtung (18) aufweist, um bei Auftreten des Verifikationssignals elektromagnetisch ein Türschloß zu entriegeln.

10. Annäherungssensitives Kontrollsystem mit einem Transponder nach einem der Ansprüche 2 und 3 sowie einer Basisstation nach einem der Ansprüche 5 und 6, wobei die Basisstation eine Entfernungsmesseinrichtung (19) zur Bestimmung der Entfernung zwischen Transponder (2) und Basisstation (1) aufweist.

11. System nach Anspruch 10, wobei die Basisstation (1) eine Steuereinheit (19) aufweist, die sie veranlaßt, wiederholt ein Abfragesignal (3) an den Transponder (2) auszusenden,

der Transponder (2) zum getakteten Abtasten des empfangenen Signals mit einer Abtastfrequenz und zum Aussenden eines Antwortsignals (4), wenn das Abfragesignal (3) abgetastet wurde, eingerichtet ist, und

die Entfernungsmesseinrichtung (19) der Basisstation (1) mit einem Taktgeber, dessen Frequenz sich von der genannten Abtastfrequenz geringfügig unterscheidet und mit einer statistischen Laufzeitermittlungseinrichtung versehen ist, die bei jeder Wiederholung des Aussendens des Abfragesignals die Anzahl der Takte des Taktgebers bis zum Empfang des Antwortsignals bestimmt und aus dem Verhältnis der Anzahl der Wiederholungen, bei denen eine größere von zwei häufigsten Taktzahlen bestimmt wurde, zur Gesamtzahl der Wiederholungen die Entfernung zwischen Basisstation (1) und Transponder (2) ermittelt.

12. Annäherungssensitives Kontrollsystem, mit einer Basisstation (1) zum drahtlosen Aussenden eines Abfragesignals (3), einem Transponder (2) zum Empfang des Abfragesignals (3) und drahtlosen Aussenden eines Antwortsignals (4), aufgrund dessen die Basisstation (1) den Transponder identifiziert, wobei die Basisstation (1) einen Zufallszahlfolgegenerator (10) enthält, der eine Zufallszahlfolge erzeugt, die in dem Abfragesignal (3) enthalten ist,

die Basisstation (1) eine erste Verschlüsselungseinrichtung (13, 14) zur Verschlüsselung der Zufallszahlfolge und Erzeugen eines ersten verschlüsselten Signals enthält, der Transponder (2) eine zweite Verschlüsselungseinrichtung (22, 23) zur Verschlüsselung der in dem empfangenen Abfragesignal (3) enthaltenen Zufallszahlfolge und Erzeugen eines zweiten verschlüsselten Signals, das in dem Antwortsignal (4) enthalten ist, enthält, und

die Basisstation eine Verifikationseinrichtung (17), zur Identifizierung des Transponders aufgrund eines Vergleichs des ersten verschlüsselten Signals mit dem in dem empfangenen Antwortsignal (4) enthaltenen zweiten verschlüsselten Signal enthält.

13. Annäherungssensitives Kontrollsystem, mit einer Basisstation (1) zum wiederholten drahtlosen Aussenden eines Abfragesignals (3), einem Transponder (2) zum Empfang und getakteten Abtasten des Abfragesignals (3) mit einer Abtastfrequenz und drahtlosen Aussenden eines Antwortsignals (4), aufgrund dessen die Basisstation (1) den Transponder identifiziert, wenn das Abfragesignal abgetastet wurde, wobei

die Basisstation (1) einen Taktgeber, dessen Frequenz sich von der genannten Abtastfrequenz geringfügig unterscheidet und eine Entfernungsmesseinrichtung (19) aufweist, die bei jeder Wiederholung des Aussendens des Abfragesignals die Anzahl der Takte des Taktgebers bis zum Empfang des Antwortsignals bestimmt und aus dem Verhältnis der Anzahl der Wiederholungen, bei denen eine größere von zwei häufigsten Taktzahlen bestimmt wurde, zur Gesamtzahl der Wiederholungen die Entfernung zwischen Basisstation (1) und Transponder (2) ermittelt.

Hierzu 3 Seite(n) Zeichnungen

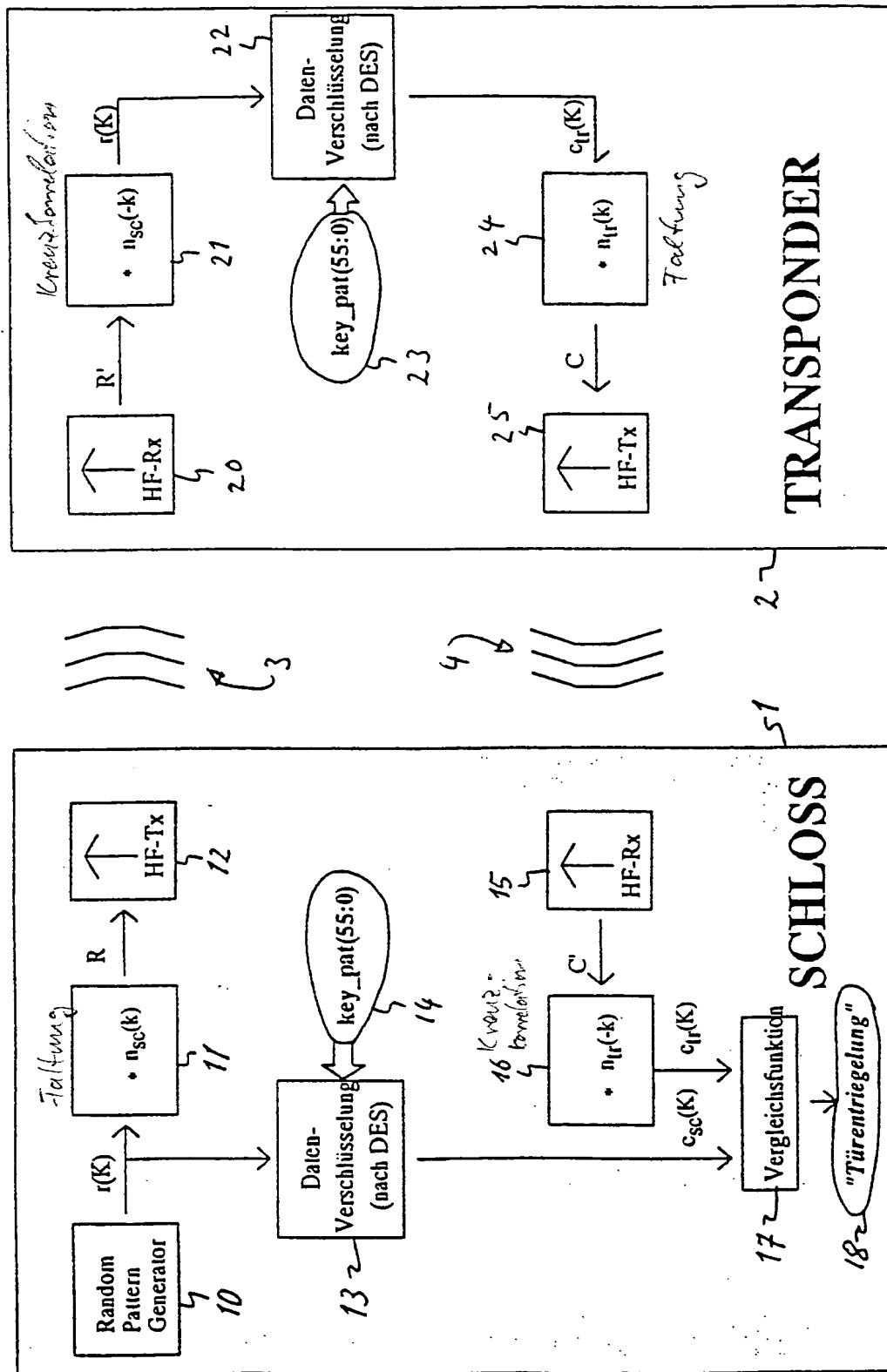


Fig. 1



BEST AVAILABLE COPY

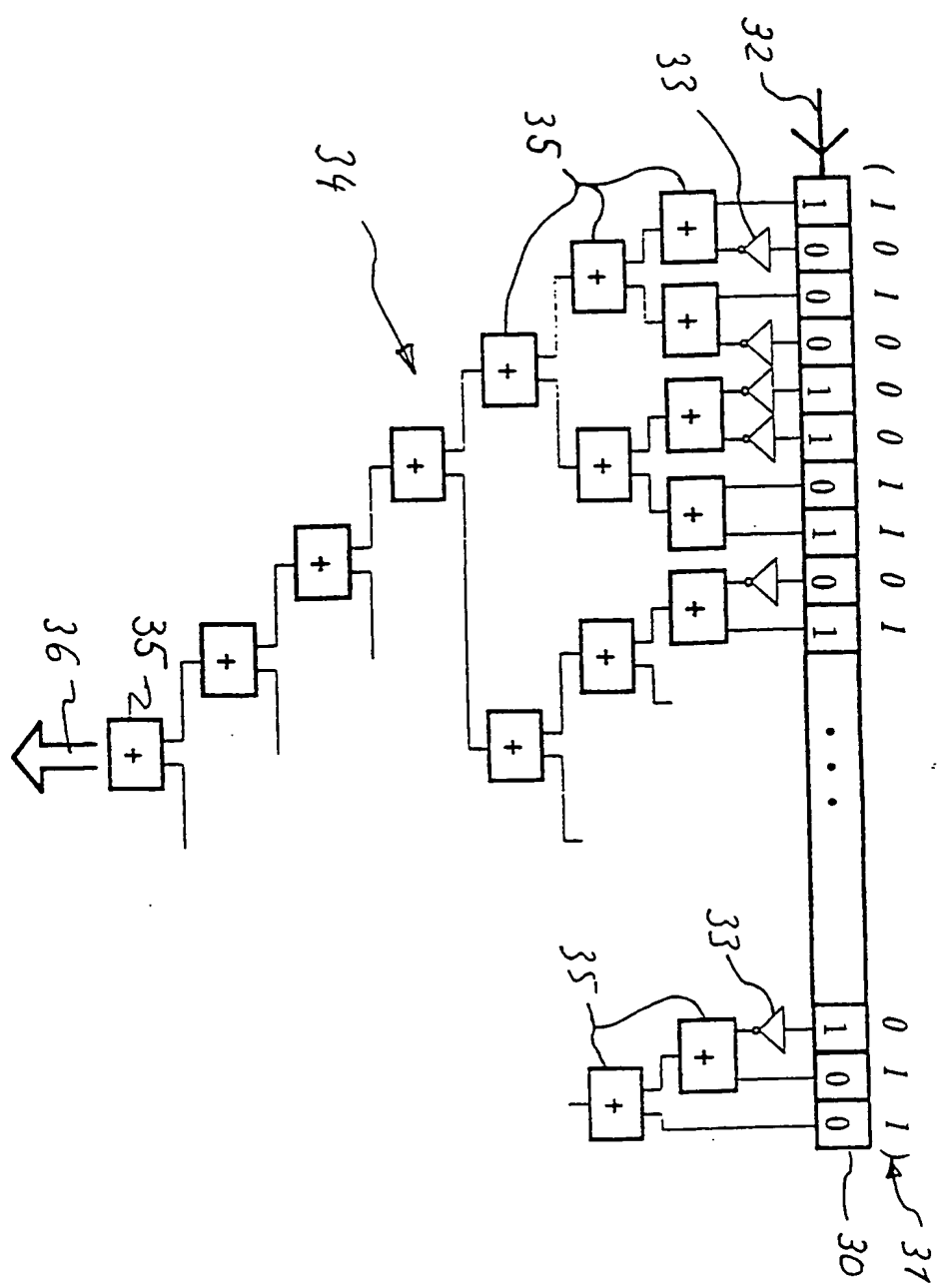


Fig. 2

Docket # 6999P/915  
 Applic. # \_\_\_\_\_  
 Applicant: Reisinger et al  
 Lerner and Greenberg, P.A.  
 Post Office Box 2480  
 Hollywood, FL 33022-2480  
 Tel: (954) 925-1100 Fax: (954) 925-1101

**Fig. 3**

